IMAGE VERIFICATION SYSTEM, IMAGE VERIFICATION DEVICE, IMAGE VERIFICATION METHOD, PROGRAM, AND RECORDING MEDIUM

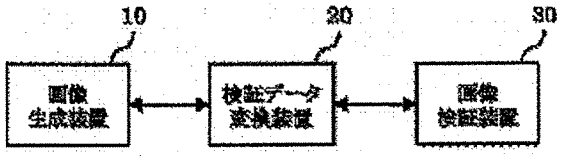
Publication number: JP2002244924
Publication date: 2002-08-30
Inventor: WAKAO SATOSHI; IWAMURA KEIICHI
Applicant: CANON KK
Classification:
- international: ***G06F12/14; G06F21/24; G09C1/00; H04L9/32; H04N1/32; H04N1/40; H04N5/225;*** *H04N101/00;* **G06F12/14; G06F21/00; G09C1/00; H04L9/32; H04N1/32; H04N1/40; H04N5/225;** (IPC1-7): G06F12/14; G09C1/00; H04L9/32; H04N1/40; H04N5/225; H04N101/00
- European: H04L9/32S; H04N1/32C17
Application number: JP20010346689 20011112
Priority number(s): JP20010346689 20011112; JP20000351529 20001117

Also published as:
EP1209847 (A1)
US2002060736 (A1)
EP1209847 (B1)
DE60123198T (T2)

Report a data error here

Abstract of **JP2002244924**

PROBLEM TO BE SOLVED: To securely detect whether image data photographed by an image generation device such as a digital camera is altered or not while preventing an increase of cost required by the image generation device. SOLUTION: The image generation device 10 generates an image file with primary verification data every time one image data is photographed. A verification data conversion device 20 generates an image file with secondary verification data (image file with digital signature) when image data in the image file with primary verification data is not altered. An image verification device 30 verifies the completeness of the image file with secondary verification data to detect whether the file is altered or not.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－244924
（P2002－244924A）
(43)公開日　平成14年８月30日(2002.8.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ	５Ｂ０１７
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｃ０２２
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ　5/225	Ｆ	５Ｃ０７７
Ｈ０４Ｎ　1/40		101:00		５Ｊ１０４
5/225		Ｈ０４Ｌ　9/00	６７５Ｂ	

審査請求　未請求　請求項の数37　ＯＬ　（全 17 頁）　最終頁に続く

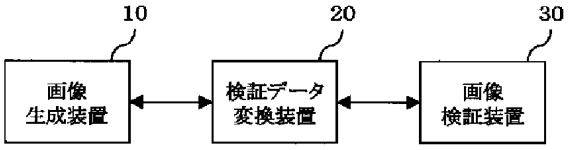
(21)出願番号　特願2001－346689(P2001－346689)
(22)出願日　平成13年11月12日(2001.11.12)
(31)優先権主張番号　特願2000－351529(P2000－351529)
(32)優先日　平成12年11月17日(2000.11.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　若尾　聡
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

最終頁に続く

(54)【発明の名称】　画像検証システム、画像検証装置、画像検証方法、プログラム及び記録媒体

(57)【要約】
【課題】　ディジタルカメラなどの画像生成装置にかかるコストの増大を防ぎつつ、画像生成装置で撮影された画像データが改変されているか否かを確実に検出する。
【解決手段】　画像生成装置１０は、１枚の画像データを撮影するごとに、１次検証データ付き画像ファイルを生成する。検証データ変換装置２０は、１次検証データ付き画像ファイル内の映像データが改変されていない場合、２次検証データ付き画像ファイル（ディジタル署名付き画像ファイル）を生成する。画像検証装置３０は、２次検証データ付き画像ファイルの完全性を検証し、そのファイルが改変されているか否かを検出する。



【特許請求の範囲】
【請求項１】　画像生成装置と、第１の画像検証装置とを備えた画像検証システムであって、
前記画像生成装置は、
画像データを生成する画像データ生成手段と、
前記画像データと、第１の情報とを用いて前記画像データの第１の検証データを生成する第１の検証データ生成手段とを備え、
前記第１の画像検証装置は、
前記画像データと、前記第１の検証データと、前記第１の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、
前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する第２の検証データ生成手段とを備えることを特徴とする画像検証システム。
【請求項２】　前記第１の検証データ生成手段は、ハッシュ関数と所定の演算とを用いて前記第１の検証データを生成することを特徴とする請求項１に記載の画像検証システム。
【請求項３】　前記第２の検証データ生成手段は、ハッシュ関数と公開鍵暗号とを用いて前記第２の検証データを生成することを特徴とする請求項１または２に記載の画像検証システム。
【請求項４】　前記第２の検証データ生成手段は、前記画像データが改変されている場合、前記第２の検証データの生成を禁止することを特徴とする請求項１～３の何れか１項に記載の画像検証システム。
【請求項５】　前記第１の画像検証装置は、前記第１の情報と前記第２の情報との対応関係を記憶したメモリを備えることを特徴とする請求項１～４の何れか１項に記載の画像検証システム。
【請求項６】　前記第１の情報は、前記画像生成装置を特定するＩＤ情報であることを特徴とする請求項１～５の何れか１項に記載の画像検証システム。
【請求項７】　前記第２の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項１～６の何れか１項に記載の画像検証システム。
【請求項８】　前記画像検証システムは更に、第２の画像検証装置を備え、前記第２の画像検証装置は、前記画像データと、前記第２の検証データと、前記第２の情報に対応する第３の情報とを用いて前記画像データが改変されているか否かを検証する検証手段を備えることを特徴とする請求項１～７の何れか１項に記載の画像検証システム。
【請求項９】　前記第２の情報は、公開鍵暗号方式の秘密鍵であり、前記第３の情報は、公開鍵暗号方式の公開鍵であることを特徴とする請求項８に記載の画像検証システム。
【請求項１０】　前記第２の画像検証装置は、前記第１の画像検証装置をクライアントとするサーバコンピュータであることを特徴とする請求項８または９に記載の画像検証システム。
【請求項１１】　前記画像生成装置は、撮像部を備えた電子機器であることを特徴とする請求項１～１０の何れか１項に記載の画像検証システム。
【請求項１２】　前記画像生成装置は、ディジタルカメラ、カメラ一体型ディジタルカメラまたはスキャナであることを特徴とする請求項１１に記載の画像検証システム。
【請求項１３】　画像生成装置と、第１の装置と、第２の装置を備えた画像検証システムであって、
前記画像生成装置は、
画像データを生成する画像データ生成手段と、
前記画像データと、第１の情報とを用いて前記画像データの第１の検証データを生成する第１の検証データ生成手段とを備え、
前記第１の装置は、
前記画像データと、前記第１の検証データとを前記第２の装置に送信する送信手段を備え、
前記第２の装置は、
前記画像データと、前記第１の検証データと、前記第１の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、
前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する第２の検証データ生成手段とを備えることを特徴とする画像検証システム。
【請求項１４】　前記第１の検証データ生成手段は、ハッシュ関数と、所定の演算とを用いて前記第１の検証データを生成することを特徴とする請求項１３に記載の画像検証システム。
【請求項１５】　前記第２の検証データ生成手段は、ハッシュ関数と、公開鍵暗号とを用いて前記第２の検証データを生成することを特徴とする請求項１３または１４に記載の画像検証システム。
【請求項１６】　前記第２の検証データ生成手段は、前記画像データが改変されている場合、前記第２の検証データの生成を禁止することを特徴とする請求項１３～１５の何れか１項に記載の画像検証システム。
【請求項１７】　前記第２の装置は、前記第１の情報と前記第２の情報との対応関係を記憶したメモリを備えることを特徴とする請求項１３～１６の何れか１項に記載の画像検証システム。
【請求項１８】　前記第１の情報は、前記画像生成装置を特定するＩＤ情報であることを特徴とする請求項１３～１７の何れか１項に記載の画像検証システム。
【請求項１９】　前記第２の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項１３～１８の何れか１項に記載の画像検証システム。

【請求項２０】　前記第２の装置は、ＩＣカードまたはマイクロプロセッサ付き記憶媒体であることを特徴とする請求項１３～１９の何れか１項に記載の画像検証システム。

【請求項２１】　前記第２の装置は、前記第１の装置をクライアントとするサーバコンピュータであることを特徴とする請求項１３～１９の何れか１項に記載の画像検証システム。

【請求項２２】　前記画像検証システムは更に、画像検証装置を備え、前記画像検証装置は、前記画像データと、前記第２の検証データと、前記第２の情報に対応する第３の情報とを用いて前記画像データが改変されているか否かを検証する検証手段を備えることを特徴とする請求項１３～２１の何れか１項に記載の画像検証システム。

【請求項２３】　前記第２の情報は、公開鍵暗号方式の秘密鍵であり、前記第３の情報は、公開鍵暗号方式の公開鍵であることを特徴とする請求項２２に記載の画像検証システム。

【請求項２４】　前記画像検証装置は、前記第１の装置をクライアントとするサーバコンピュータであることを特徴とする請求項２２または２３に記載の画像検証システム。

【請求項２５】　前記画像生成装置は、撮像部を備えた電子機器であることを特徴とする請求項１３～２４の何れか１項に記載の画像検証システム。

【請求項２６】　前記画像生成装置は、ディジタルカメラ、カメラ一体型ディジタルカメラまたはスキャナであることを特徴とする請求項２５に記載の画像検証システム。

【請求項２７】　画像データと、前記画像データの第１の検証データと、第１の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、
前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する生成手段とを備えることを特徴とする画像検証装置。

【請求項２８】　前記生成手段は、ハッシュ関数と公開鍵暗号とを用いて前記第２の検証データを生成することを特徴とする請求項２７に記載の画像検証装置。

【請求項２９】　前記第２の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項２７または２８に記載の画像検証装置。

【請求項３０】　前記生成手段は、前記画像データが改変されている場合、前記第２の検証データの生成を禁止することを特徴とする請求項２７～２９の何れか１項に記載の画像検証装置。

【請求項３１】　前記画像検証装置は、前記第１の情報と前記第２の情報との対応関係を記憶したメモリを備えることを特徴とする請求項２７～３０の何れか１項に記載の画像検証装置。

【請求項３２】　画像データと、前記画像データの第１の検証データと、第１の情報とを用いて前記画像データが改変されているか否かを検証する検証ステップと、
前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する生成ステップとを有することを特徴とする画像検証方法。

【請求項３３】　前記検証データ生成ステップは、ハッシュ関数と公開鍵暗号とを用いて前記第２の検証データを生成することを特徴とする請求項３２に記載の画像検証方法。

【請求項３４】　前記第２の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項３２または３３に記載の画像検証方法。

【請求項３５】　前記生成ステップは、前記画像データが改変されている場合、前記第２の検証データの生成を禁止することを特徴とする請求項３２～３４の何れか１項に記載の画像検証方法。

【請求項３６】　請求項３２～３５の何れか１項に記載の画像検証方法をコンピュータに実行させるためのプログラム。

【請求項３７】　請求項３６に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタルカメラなどの画像生成装置で生成された画像データの改変を検出する画像検証システム、画像生成装置、画像生成方法、プログラム及び記録媒体に関するものである。

【０００２】

【従来の技術】近年、被写体の光学像をディジタル化して記憶するディジタルカメラが実用化されている。ディジタルカメラで撮影された画像データは、パーソナルコンピュータに取り込むことが簡単にできる反面、パーソナルコンピュータ上で簡単に改変することができるという問題があった。そのため、ディジタルカメラで撮影された画像データの信頼性は、銀塩写真よりも低く、証拠能力が乏しいという問題があった。そこで、近年、ディジタルカメラで撮影された画像データにディジタル署名を付加する機能を備えたディジタルカメラシステムが提案されている。従来のディジタル署名機能付きディジタルカメラシステムは、例えば、米国特許第５，４９９，２９４、特開平９－２００７３０号などに開示されている。

【０００３】

【発明が解決しようとする課題】ディジタル署名の生成には、通常、ＲＳＡ暗号などの公開鍵暗号方式が利用される。しかしながら、ＲＳＡ暗号などの公開鍵暗号方式は、べき乗演算や剰余演算が必要であるために高速な処

理が難しく、ＤＥＳなどの共通鍵暗号方式に比べて数百倍から数千倍の処理時間が必要である。そのため、従来のディジタルカメラの限られた演算リソースでは、ディジタル署名の生成が大変難しいという問題があった。ディジタルカメラの演算リソースの性能を大幅に向上させ、ディジタル署名の生成を容易に行えるようにする方法もあるが、このような方法ではディジタルカメラ本体にかかるコストが非常に増大してしまうため好ましくない。

【０００４】本発明は、上述の問題点に鑑みてなされたものであり、ディジタルカメラなどの画像生成装置にかかるコストの増大を防ぎつつ、画像生成装置で撮影された画像データが改変されているか否かを確実に検出することのできる画像検証システム、画像検証装置、画像検証方法、プログラム及び記録媒体を提供することを目的とする。

【０００５】

【課題を解決するための手段】本発明の画像検証システムは、画像生成装置と、第１の画像検証装置とを備えた画像検証システムであって、前記画像生成装置は、画像データを生成する画像データ生成手段と、前記画像データと、第１の情報とを用いて前記画像データの第１の検証データを生成する第１の検証データ生成手段とを備え、前記第１の画像検証装置は、前記画像データと、前記第１の検証データと、前記第１の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する第２の検証データ生成手段とを備えることを特徴とする。

【０００６】また、本発明の画像検証システムは、画像生成装置と、第１の装置と、第２の装置を備えた画像検証システムであって、前記画像生成装置は、画像データを生成する画像データ生成手段と、前記画像データと、第１の情報とを用いて前記画像データの第１の検証データを生成する第１の検証データ生成手段とを備え、前記第１の装置は、前記画像データと、前記第１の検証データとを前記第２の装置に送信する送信手段を備え、前記第２の装置は、前記画像データと、前記第１の検証データと、前記第１の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、前記画像データが改変されていない場合、前記画像データと第２の情報とを用いて前記画像データの第２の検証データを生成する第２の検証データ生成手段とを備えることを特徴とする。

【０００７】また、本発明の画像検証装置は、画像データと、前記画像データの第１の検証データと、第１の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する生成手段とを備えることを特徴とする。

【０００８】また、本発明の画像検証方法は、画像データと、前記画像データの第１の検証データと、第１の情報とを用いて前記画像データが改変されているか否かを検証する検証ステップと、前記画像データが改変されていない場合、前記画像データと、第２の情報とを用いて前記画像データの第２の検証データを生成する生成ステップとを有することを特徴とする。

【０００９】

【発明の実施の形態】（第１の実施の形態）以下、図面を参照し、本発明に好適な第１の実施の形態について説明する。まず、図１２を参照し、第１の実施の形態における画像データ検証システムの構成の一例を説明する。

【００１０】１０は、被写体の画像データと、その画像データの完全性を検証するための１次検証データとを生成し、１次検証データ付き画像ファイルを生成する画像生成装置である。なお、画像生成装置１０は、ディジタルカメラ、カメラ一体型ディジタルビデオレコーダ、スキャナなどの撮像装置であっても、被写体の画像データを撮影する機能を備えた電子機器であってもよい。

【００１１】２０は、１次検証データ付き画像ファイル内の画像データの完全性を検証し、その画像データが改変されているか否かを検出する検証データ変換装置である。また、検証データ変換装置２０は、その画像データの完全性が確認された場合（即ち、その画像データが改変されていない場合）、その画像データの完全性及び正当性を検証するための２次検証データ（即ち、ディジタル署名）を生成し、１次検証データ付き画像ファイルを２次検証データ付き画像ファイルに変換する。なお、検証データ変換装置２０は、パーソナルコンピュータなどのコンピュータである。

【００１２】３０は、２次検証データ付き画像ファイル内の画像データの完全性を検証し、その画像データが改変されているか否かを検出する画像検証装置である。なお、画像検証装置３０は、パーソナルコンピュータなどのコンピュータであっても、検証データ変換装置２０をクライアントとするサーバコンピュータであってもよい。

【００１３】画像生成装置１０と検証データ変換装置２０との間は、ＬＡＮ、ＩＥＥＥ１３９４－１９９５、ＵＳＢ（Universal Serial Bus）などのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。また、検証データ変換装置２０と画像検証装置３０との間を接続する媒体は、ＬＡＮ、ＷＡＮ、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。

【００１４】次に、第１の実施の形態における画像生成

装置１０の構成について説明する。図１は、第１の実施の形態における画像生成装置１０の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

【００１５】１１は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。１４は、ＣＣＤ（電荷結合素子）などの光学センサーを含む撮像部である。１５は、１次検証データ付き画像ファイルを記憶する保管用メモリである。１６は、１次検証データ付き画像ファイルを検証データ変換装置２０に送信するインターフェース部である。１７は、プログラムメモリである。プログラムメモリ１７は、１次検証データ付き画像ファイルを生成する機能を制御するプログラムを記憶している。また、プログラムメモリ１７は、１次検証データの生成に必要な共通情報Ｋｃ（これは、共通鍵暗号方式の暗号鍵に相当する）と、画像生成装置１０の固有ＩＤ（画像生成装置１０だけを特定可能な識別子であればよい。例えば、製造番号、シリアル番号など）とを記憶している。なお、プログラムメモリ１７は、ＲＯＭであっても、ＥＥＰＲＯＭであってもよい。但し、プログラムメモリ１７内の情報は、外部に漏れないように秘密に管理するものとする。１８は、ユーザからの様々な指示（撮影の開始など）を受け付ける操作部である。

【００１６】次に、第１の実施の形態における検証データ変換装置２０の構成について説明する。図２は、第１の実施の形態における検証データ変換装置２０の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

【００１７】２１は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。２４は、画像生成装置１０からの１次検証データ付き画像ファイルを受信するインターフェース部Ａである。２８は、画像検証装置３０に２次検証データ付き画像ファイルを送信するインターフェース部Ｂである。２５は、１次検証データ付き画像ファイル及び２次検証データ付き画像ファイルを記憶する保管用メモリである。２６は、プログラムメモリである。プログラムメモリ２６は、１次検証データ付き画像ファイルの完全性を検証する機能と、２次検証データ付き画像ファイルを生成する機能とを制御するプログラムを記憶している。また、プログラムメモリ２６は、複数の画像生成装置の固有ＩＤと、各固有ＩＤに対応する共通情報Ｋｃ（これは、共通鍵暗号方式の復号鍵に相当する）と、各固有ＩＤに対応する秘密情報Ｋｓ（これは、公開鍵暗号方式の秘密鍵に相当する）とを登録したテーブルＴ１を記憶している。テーブルＴ１の一例を図７（ａ）に示す。なお、プログラムメモリ２６は、ＲＯＭであっても、ＥＥＰＲＯＭであってもよい。但し、プログラムメモリ２６内の情報は、外部に漏れないように秘密に管理するものとする。２７は、ユーザからの様々な指示を受け付ける操作部である。２２は、２次検証データ付き画像ファイルの画像データが改変されているか否かを示すメッセージをディスプレイ装置、プリンタなどの外部装置に出力する出力部である。

【００１８】次に、第１の実施の形態における画像検証装置３０の構成について説明する。図３は、第１の実施の形態における画像検証装置３０の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

【００１９】３１は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。３４は、２次検証データ付き画像ファイルを受信したり、２次検証データ付き画像ファイルの完全性を検証するときに必要な公開情報Ｋｐを受信したりするインターフェース部である。３６は、プログラムメモリである。プログラムメモリ３６は、２次検証データ付き画像ファイルの完全性を検証する機能を制御するプログラムを記憶している。また、プログラムメモリ３６は、複数の画像生成装置の固有ＩＤと、各固有ＩＤに対応する公開情報Ｋｐ（これは、公開鍵暗号方式の公開鍵に相当する）とを登録したテーブルＴ２を記憶している。テーブルＴ２の一例を図７（ｂ）に示す。なお、プログラムメモリ３６は、ＲＯＭであっても、ＥＥＰＲＯＭであってもよい。３７は、ユーザからの様々な指示を受け付ける操作部である。３２は、２次検証データ付き画像ファイルに改変があるか否かを示すメッセージをディスプレイ装置、プリンタなどの外部装置に出力する出力部である。３５は、２次検証データ付き画像ファイルを記憶する保管用メモリである。また、保管用メモリ３５は、改変の有無、登録日時、検証日時などの情報を登録するデータベースを有する。

【００２０】次に、第１の実施の形態における画像データ検証システムの処理手順について説明する。図４は、第１の実施の形態における画像データ検証システムの処理手順について説明する図である。

【００２１】ステップＳ４０１：画像生成装置１０は、ユーザの撮影指示に従って被写体の画像データを生成し、生成された画像データを所定の画像ファイルフォーマットに準拠した画像ファイルにファイル化する。このとき、画像データは、所定の画像ファイルフォーマットに準拠した画像圧縮符号化方式に従って圧縮符号化される。なお、所定の画像ファイルフォーマットは、ＪＦＩＦ（JPEG File Interchange Format）、ＴＩＦＦ（Tagged Image File Format）及びＧＩＦ（Graphics Interchange Format）の何れかであっても、それらを拡張したものであっても、他の画像ファイルフォーマットであってもよい。

【００２２】ステップＳ４０２：画像生成装置１０は、生成された画像データと共有情報Ｋｃとからその画像データの１次検証データを生成する。

【００２３】図５（ａ）及び図５（ｂ）を参照し、１次検証データの生成方法の一例を説明する。なお、１次検証データの生成方法は、１次検証データの安全のために、一般には公開されないものであり、画像生成装置１０の内部及び検証データ変換装置２０の内部で秘密に管理されるものである。

【００２４】図５（ａ）は、１次検証データの第１の生成方法について説明する図である。図５（ａ）に示す第１の生成方法は、以下の（ａ１）～（ａ３）に示す手順に従って実行される。なお、図５（ａ）に示す生成方法は、画像生成装置１０の制御／演算部１１及び検証データ変換装置２０の制御／演算部２１で実行される。

【００２５】（ａ１）まず、簡易な演算を実行し、画像データを共有情報Ｋｃで暗号化する。簡易な演算の一例を図６に示す。第１の実施の形態では、図６に示すように、画像データの一部（例えば、最上位バイト）と共有情報Ｋｃ（例えば、「１１１１１１１１」）との間で排他的論理和演算を行い、画像データを暗号化する。なお、簡易な演算は、画像生成装置１０の限られた演算リソース上で高速に実行できるものであれば、他の演算アルゴリズムに置き換えてもよい。

【００２６】（ａ２）次に、（ａ１）で得られたデータをハッシュ関数Ｈ１によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数Ｈ１は、ＭＤ－２、ＭＤ－４、ＭＤ－５、ＳＨＡ－１、ＲＩＰＥＭＤ－１２８及びＲＩＰＥＭＤ－１６０の何れかであっても、他のハッシュ関数であってもよい。

【００２７】（ａ３）最後に、（ａ２）で得られたダイジェストデータを１次検証データとする。

【００２８】図５（ｂ）は、１次検証データの第２の生成方法について説明する図である。図５（ｂ）に示す生成方法は、以下の（ｂ１）～（ｂ３）に示す手順に従って実行される。なお、図５（ｂ）に示す第２の生成方法は、画像生成装置１０の制御／演算部１１及び検証データ変換装置２０の制御／演算部２１で実行される。

【００２９】（ｂ１）まず、画像データをハッシュ関数Ｈ１によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数Ｈ１は、ＭＤ－２、ＭＤ－４、ＭＤ－５、ＳＨＡ－１、ＲＩＰＥＭＤ－１２８及びＲＩＰＥＭＤ－１６０の何れかであっても、他のハッシュ関数であってもよい。

【００３０】（ｂ２）次に、所定の共通鍵暗号方式に従ってダイジェストデータを共有情報Ｋｃで暗号化する。なお、所定の共通鍵暗号方式は、ＤＥＳまたはＲｉｎｊｄａｅｌであっても、他の共通鍵暗号方式であってもよい。

【００３１】（ｂ３）最後に、共有情報Ｋｃで暗号化されたダイジェストデータを１次検証データとする。

【００３２】ステップＳ４０３：画像生成装置１０は、生成された１次検証データを画像ファイルのヘッダ部に付加し、１次検証データ付き画像ファイルを生成する。また、画像生成装置１０は、１次検証データだけでなく、画像生成装置１０の固有ＩＤも画像ファイルのヘッダ部に付加する。

【００３３】ステップＳ４０４：画像生成装置１０は、１次検証データ付き画像ファイルを検証データ変換装置２０に送信する。

【００３４】ステップＳ４０５：１次検証データ付き画像ファイルを受信した後、検証データ変換装置２０は、そのファイルのヘッダ部から１次検証データ及び画像生成装置１０の固有ＩＤを抽出し、そのファイルのデータ部から画像データを抽出する。また、検証データ変換装置２０は、プログラムメモリ２６内のテーブルＴ１を参照し、抽出された固有ＩＤに対応する共有情報Ｋｃ及び秘密情報Ｋｓを検出する。例えば、画像生成装置１０の固有ＩＤが「００１」である場合、その固有ＩＤに対応する共有情報Ｋｃは「０ｘ１１１１」であり、その固有ＩＤに対応する秘密情報Ｋｓは「０ｘ２２２２」である。検証データ変換装置２０は、抽出された画像データと検出された共有情報Ｋｃとからその画像データの１次検証データを生成する。なお、検証データ変換装置２０は、画像生成装置１０と同じ生成方法に従って１次検証データを生成する。

【００３５】ステップＳ４０６：検証データ変換装置２０は、１次検証データ付き画像ファイルから抽出された１次検証データ（即ち、画像生成装置１０の内部で生成された１次検証データ）と、ステップＳ４０５で生成された１次検証データ（即ち、検証データ変換装置２０の内部で生成された１次検証データ）とを比較し、１次検証データ付き映像ファイル内の画像データの完全性を検証する。画像生成装置１０から検証データ変換装置２０に至るまでに改変がなかった場合、２つの１次検証データは一致する。この場合、検証データ変換装置２０は、この画像データが画像生成装置１０で生成された画像データであり、改竄のない安全な画像データであることを確実に確認することができる。更にこの場合、検証データ変換装置２０は、改変なしと判定し、この画像データの２次検証データの生成を開始する。一方、画像生成装置１０から検証データ変換装置２０に至るまでに改変があった場合、２つの１次検証データは一致しない。この場合、検証データ変換装置２０は、改変ありと判定し、この画像データが改変されていることを示すメッセージをユーザに通知する。なお、この場合、検証データ変換装置２０は、この画像データの２次検証データの生成を禁止する。

【００３６】ステップＳ４０７：改変なしと判定した場合、検証データ変換装置２０は、１次検証データ付き画像ファイル内の画像データから２次検証データ（即ち、ディジタル署名）を生成する。

【００３７】図８を参照し、２次検証データの生成方法

を説明する。図８に示す生成方法は、以下の（１）～（３）に示す手順に従って実行される。なお、図８に示す生成方法は、検証データ変換装置２０の制御／演算部２１及び画像検証装置３０の制御／演算部３１で実行される。

【００３８】（１）まず、画像データをハッシュ関数Ｈ２によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数Ｈ２は、ＭＤ－２、ＭＤ－４、ＭＤ－５、ＳＨＡ－１、ＲＩＰＥＭＤ－１２８及びＲＩＰＥＭＤ－１６０の何れかであっても、他のハッシュ関数であってもよい。

【００３９】（２）次に、所定の公開鍵暗号方式に従ってダイジェストデータを秘密情報Ｋｓで暗号化する。なお、所定の公開鍵暗号方式は、ＲＳＡ暗号方式であっても、他の公開鍵暗号方式であってもよい。

【００４０】（３）最後に、秘密情報Ｋｓで暗号化されたダイジェストデータを２次検証データ（即ち、ディジタル署名）とする。

【００４１】ステップＳ４０８：検証データ変換装置２０は、画像ファイルのヘッダ部にある１次検証データを２次検証データに置き換え、２次検証データ付き画像ファイルを生成する。生成された２次検証データ付き画像ファイルは、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力される。画像検証装置３０は、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）から２次検証データ付き画像ファイルを入力する。

【００４２】ステップＳ４０９：２次検証データ付き画像ファイルを入力した後、画像検証装置３０は、そのファイルのヘッダ部から２次検証データ及び画像生成装置１０の固有ＩＤを抽出する。また、画像検証装置３０は、プログラムメモリ３６内のテーブルＴ２を参照し、抽出された固有ＩＤに対応する公開情報Ｋｐを検出する。例えば、画像生成装置１０の固有ＩＤが「００１」の場合、その固有ＩＤに対応する公開情報Ｋｐは「０ｘ３３３３」である。なお、公開情報Ｋｐは、所定のサーバから取得してもよい。画像検証装置３０は、抽出された２次検証データを検出された公開情報Ｋｐで復号化し、ダイジェストデータ（ハッシュ値）を復元する。なお、公開情報Ｋｐは、検証データ変換装置２０が秘密に管理している秘密情報Ｋｓに対応する情報であり、一般に公開されている情報である。

【００４３】ステップＳ４１０：また、画像検証装置３０は、２次検証データ付き画像ファイルのデータ部から画像データを抽出する。画像検証装置３０は、抽出された画像データをハッシュ関数Ｈ２によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数Ｈ２は、検証データ変換装置２０のハッシュ関数Ｈ２と同じハッシュ関数である。

【００４４】ステップＳ４１１：画像検証装置３０は、ステップＳ４０９で復元されたダイジェストデータと、ステップＳ４１０で得られたダイジェストデータとを比較し、２次検証データ付き映像ファイル内の画像データの完全性及び正当性を検証する。検証データ変換装置２０から画像検証装置３０に至るまでに改変がなかった場合、２つのダイジェストデータは一致する。この場合、２次検証装置３０は、この画像データが画像生成装置１０で生成された画像データであることと、この画像データの２次検証データは１次検証装置２０で付加されたものであることを確実に確認することができる。更にこの場合、画像検証装置３０は、改変なしと判定し、その判定結果をユーザに通知する。一方、検証データ変換装置２０から画像検証装置３０に至るまでに改変があった場合、２つのダイジェストデータは一致しない。この場合、画像検証装置３０は、改変ありと判定し、その判定結果をユーザに通知する。

【００４５】ステップＳ４１２：画像検証装置３０は、２次検証データ付き画像ファイルの改変をチェックするごとに、画像ファイルのファイル名、画像ファイルの登録日時、画像ファイルの検証日時、改変の有無などの情報を保管用メモリ３５のデータベースに登録する。このような情報を保管用メモリに登録することで、検証者は、検証された２次検証データ付き画像ファイルを管理することができる。

【００４６】以上説明したように、第１の実施の形態における画像データ検証システムによれば、画像生成装置１０の演算リソースの性能を大幅に向上させることなく、画像生成装置１０で生成された画像データが改変されているか否かを確実に検出することができる。

【００４７】また、第１の実施の形態における画像データ検証システムによれば、画像生成装置１０にかかるコストを低減することができる。また、第１の実施の形態における画像データ検証システムによれば、画像生成装置１０の固有ＩＤに対応する共有情報Ｋｃ、秘密情報Ｋｓ及び公開情報Ｋｐを用いて１次検証データ及び２次検証データを検証することにより、１次検証データ付き画像ファイル内の画像データまたは２次検証データ付き画像ファイル内の画像データが画像生成装置１０で生成されたものであるか否かを確実に確認することができる。

【００４８】また、第１の実施の形態における画像データ検証システムによれば、画像生成装置１０と検証データ変換装置２０との間を１次検証データによって安全に保護することができ、検証データ変換装置２０と画像検証装置３０との間を２次検証データ（即ち、ディジタル署名）によって安全に保護することができるので、システム全体の安全に運用することができる。

【００４９】次に、図９のフローチャートを参照し、第１の実施の形態における画像生成装置１０の処理手順について説明する。なお、図９に示す処理手順は、プログ

ラムメモリ１７のプログラムに従って実行される。また、図９に示す処理手順は、１枚の画像データを撮像するごとに実行される。

【００５０】ステップＳ９１：撮像部１４は、ユーザの指示に従って被写体の画像データを生成する。制御／演算部１１は、撮像部１４で生成された画像データを所定の画像ファイルフォーマットに準拠した画像ファイルにファイル化する。

【００５１】ステップＳ９２：制御／演算部１１は、生成された画像データと共有情報Ｋｃとからその画像データの１次検証データを生成する。

【００５２】ステップＳ９３：制御／演算部１１は、生成された１次検証データを画像ファイルのヘッダ部に付加し、１次検証データ付き画像ファイルを生成する。また、制御／演算部１１は、１次検証データだけでなく、画像生成装置１０の固有ＩＤ情報（即ち、固有ＩＤ）も画像ファイルのヘッダ部に付加する。

【００５３】ステップＳ９４：インターフェース部１６は、１次検証データ付き画像ファイルを外部に出力する。

【００５４】以上の処理手順により、画像生成装置１０は、１つの画像データを生成するごとに、その画像データの１次検証データを生成し、画像データとその１次検証データと画像生成装置１０の固有ＩＤとを１つの画像ファイルにファイル化することができる。

【００５５】次に、図１０のフローチャートを参照し、第１の実施の形態における検証データ変換装置２０の処理手順について説明する。なお、図１０に示す処理手順は、プログラムメモリ２６のプログラムに従って実行される。また、図１０に示す処理手順は、１次検証データ付き画像ファイルを入力するごとに実行される。

【００５６】ステップＳ１０１：インターフェース部２４は、外部から１次検証データ付き画像ファイルを入力する。

【００５７】ステップＳ１０２：制御／演算部２１は、１次検証データ付き画像ファイルのヘッダ部から１次検証データを抽出する。

【００５８】ステップＳ１０３：また、制御／演算部２１は、１次検証データ付き画像ファイルのヘッダ部から画像生成装置１０の固有ＩＤを抽出し、そのファイルのデータ部から画像データを抽出する。制御／演算部２１は、プログラムメモリ２６内のテーブルＴ１を参照し、抽出された固有ＩＤに対応する共有情報Ｋｃ及び秘密情報Ｋｓを検出する。制御／演算部２１は、抽出された画像データと検出された共有情報Ｋｃとからその画像データの１次検証データを生成する。

【００５９】ステップＳ１０４：ステップＳ１０２で抽出された１次検証データ（即ち、画像生成装置１０の内部で生成された１次検証データ）と、ステップＳ１０３で生成された１次検証データ（即ち、検証データ変換装置２０の内部で生成された１次検証データ）とを比較し、画像データの完全性を検証する。２つの１次検証データの一致が検出された場合、ステップＳ１０５に進む。一方、２つの１次検証データの一致が検出されなかった場合、ステップＳ１０６に進む。

【００６０】ステップＳ１０５：この場合、制御／演算部２１は、改変ありと判定し、画像データが改変されていることを示すメッセージをユーザに通知する。なお、この場合、画像生成装置１０は、２次検証データの生成を禁止する。

【００６１】ステップＳ１０６：この場合、制御／演算部２１は、１次検証データ付き画像ファイル内の画像データから２次検証データ（即ち、ディジタル署名）を生成する。

【００６２】ステップＳ１０７：制御／演算部２１は、画像ファイルのヘッダ部にある１次検証データを生成された２次検証データに置き換え、２次検証データ付き画像ファイルを生成する。生成された２次検証データ付き画像ファイルは、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力される。

【００６３】以上の処理手順により、検証データ変換装置２０は、画像生成装置１０の演算リソースの性能を大幅に向上させることなく、画像生成装置１０で生成された画像データが改変されているか否かを確実に検出することができる。また、検証データ変換装置２０は、１次検証データ付き画像ファイルの画像データが画像生成装置１０で生成されたものであるか否かを確実に確認することができる。また、１次検証データ付き画像ファイルの完全性が確認できれば、そのファイルを２次検証データ付き画像ファイル（即ち、ディジタル署名付き画像ファイル）に変換することもできる。

【００６４】次に、図１１のフローチャートを参照し、第１の実施の形態における画像検証装置３０の処理手順について説明する。なお、図１１に示す処理手順は、プログラムメモリ３６のプログラムに従って実行される。また、図１１に示す処理手順は、２次検証データ付き画像ファイルを入力するごとに実行される。

【００６５】ステップＳ１１１：インターフェース部３４は、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）から２次検証データ付き画像ファイルを入力する。

【００６６】ステップＳ１１２：画像検証装置３０は、２次検証データ付き画像ファイルのヘッダ部から画像生成装置１０の固有ＩＤを抽出する。また、画像検証装置３０は、プログラムメモリ３６内のテーブルＴ２を参照し、抽出された固有ＩＤに対応する公開情報Ｋｐを検出する。なお、公開情報Ｋｐは、所定のサーバから取得してもよい。

【００６７】ステップＳ１１３：制御／演算部３１は、２次検証データ付き画像ファイルのヘッダ部から２次検証データを抽出する。

【００６８】ステップＳ１１４：制御／演算部３１は、ステップＳ１１３で抽出された２次検証データを公開情報Ｋｐで復号化し、ダイジェストデータ（ハッシュ値）を復元する。

【００６９】ステップＳ１１５：制御／演算部３１は、２次検証データ付き画像ファイルのデータ部から画像データを抽出し、抽出された画像データをハッシュ関数Ｈ２によってダイジェストデータ（ハッシュ値）に変換する。

【００７０】ステップＳ１１６：制御／演算部３１は、ステップＳ１１４で復元されたダイジェストデータと、ステップＳ１１５で得られたダイジェストデータとを比較し、画像データの完全性及び正当性を検証する。２つのダイジェストデータの一致が検出された場合には、ステップＳ１１８に進む。一方、２つのダイジェストデータの一致が検出されなかった場合には、ステップＳ１１７に進む。

【００７１】ステップＳ１１７：この場合、制御／演算部３１は、改変ありと判定し、画像データが改変されていることを示すメッセージをユーザに通知する。

【００７２】ステップＳ１１８：この場合、制御／演算部３１は、改変なしと判定し、画像データが改変されていないことを示すメッセージをユーザに通知する。

【００７３】ステップＳ１１９：制御／演算部３１は、画像ファイルのファイル名、画像ファイルの登録日時、画像ファイルの検証日時、改変の有無などの情報を保管用メモリ３５のデータベースに登録する。

【００７４】以上の処理手順により、画像検証装置３０は、画像生成装置１０で生成された画像データが改変されているか否かを確実に検出することができる。また、画像検証装置３０は、２次検証データ付き画像ファイルの画像データが画像生成装置１０で生成されたものであるか否かを確実に確認することができる。

【００７５】以上説明したように、第１の実施の形態における画像データ検証システムによれば、画像生成装置１０の演算リソースの性能を大幅に向上させることなく、画像生成装置１０で生成された画像データが改変されているか否かを確実に検出することができる。

【００７６】（第２の実施の形態）以下、図面を参照し、本発明に好適な第２の実施の形態について説明する。第２の実施の形態では、第１の実施の形態の検証データ変換装置２０を２つのデータ処理装置によって構成し、共有情報Ｋｃ及び秘密情報Ｋｓの安全性を向上させる場合について説明する。

【００７７】まず、図１３を参照し、第２の実施の形態における画像データ検証システムの構成の一例を説明する。なお、画像生成装置１０及び画像検証装置３０の構成及びそれらが実行する処理手順は、第１の実施の形態と同じであるので、第２の実施の形態ではその説明を省略する。

【００７８】２０Ａは、第１の検証データ変換装置である。２０Ｂは、第１の検証データ変換装置２０Ａよりも外部からの攻撃に強い第２の検証データ変換装置である。検証データ変換装置２０Ａは、画像生成装置１０からの１次検証データ付き画像ファイルを検証データ変換装置２０Ｂに転送し、検証データ変換装置２０Ｂの検証結果をユーザに通知する。検証データ変換装置２０Ｂは、１次検証データ付き画像ファイル内の画像データの完全性を検証し、その画像データが改変されているか否かを検出する。また、検証データ変換装置２０Ｂは、その画像データの完全性が確認された場合（即ち、その画像データが改変されていない場合）、その画像データの完全性及び正当性を検証するための２次検証データ（即ち、ディジタル署名）を生成し、１次検証データ付き画像ファイルを２次検証データ付き画像ファイルに変換する。なお、検証データ変換装置２０Ａは、パーソナルコンピュータなどのコンピュータである。検証データ変換装置２０Ｂは、ＩＣカードなどのマイクロプロセッサ付き記憶媒体であっても、検証データ変換装置２０Ａをクライアントとするサーバコンピュータであってもよい。検証データ変換装置２０Ａがクライアントで、検証データ変換装置２０Ｂがサーバである場合、これらの装置の間の接続は、ＬＡＮ、ＷＡＮ、インターネットなどのネットワークであればよい。

【００７９】画像生成装置１０と検証データ変換装置２０Ａとの間は、ＬＡＮ、ＩＥＥＥ１３９４－１９９５、ＵＳＢ（Universal Serial Bus）などの伝送媒体、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。また、検証データ変換装置２０Ａと画像検証装置３０との間は、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。

【００８０】次に、第２の実施の形態における検証データ変換装置２０Ａの構成について説明する。図１４は、第２の実施の形態における検証データ変換装置２０Ａの主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

【００８１】１４２１は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。１４２３は、画像生成装置１０からの１次検証データ付き画像ファイルを受信するインターフェース部Ａである。１４２４は、検証データ変換装置２０Ａに１次検証データ付き画像ファイルを送信したり、検証データ変換装置２０Ａからの２次検証データ付き画像ファイルを受信したりするインターフェース部Ｂである。１４２８は、画像検証装

置３０に２次検証データ付き画像ファイルを送信するインターフェース部Ｃである。１４２５は、１次検証データ付き画像ファイル及び２次検証データ付き画像ファイルを記憶する保管用メモリである。１４２６は、プログラムメモリである。プログラムメモリ１４２６は、１次検証データ付き画像ファイルの完全性を検証する機能を制御するプログラムを記憶している。なお、プログラムメモリ１４２６は、ＲＯＭであっても、ＥＥＰＲＯＭであってもよい。１４２７は、ユーザからの様々な指示を受け付ける操作部である。１４２２は、２次検証データ付き画像ファイルに改変があるか否かを示すメッセージをディスプレイ装置、プリンタなどの外部装置に出力する出力部である。

【００８２】次に、第２の実施の形態における検証データ変換装置２０Ｂの構成について説明する。図１５は、第２の実施の形態における第２の検証データ変換装置の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

【００８３】１５２１は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。１５２４は、検証データ変換装置２０Ａからの１次検証データ付き画像ファイルを受信したり、検証データ変換装置２０Ａに２次検証データ付き画像ファイルを送信したりするインターフェース部である。１５２５は、１次検証データ付き画像ファイル及び２次検証データ付き画像ファイルを記憶する保管用メモリである。１５２６は、プログラムメモリである。プログラムメモリ１５２６は、２次検証データ付き画像ファイルを生成する機能を制御するプログラムを記憶している。また、プログラムメモリ１５２６は、複数の画像生成装置の固有ＩＤと、各固有ＩＤに対応する共通情報Ｋｃ（これは、共通鍵暗号方式の復号鍵に相当する）と、各固有ＩＤに対応する秘密情報Ｋｓ（これは、公開鍵暗号方式の秘密鍵に相当する）とを登録したテーブルＴ１を記憶している。テーブルＴ１の一例を図７（ａ）に示す。なお、プログラムメモリ１５２６は、ＲＯＭであっても、ＥＥＰＲＯＭであってもよい。但し、プログラムメモリ１５２６内の情報は、外部に漏れないように秘密に管理するものとする。

【００８４】次に、第２の実施の形態における画像データ検証システムの処理手順について説明する。図１６は、第２の実施の形態における画像データ検証システムの処理手順について説明する図である。

【００８５】ステップＳ１６０１からステップＳ１６０３までの処理手順は、第１の実施の形態のステップＳ４０１からステップＳ４０３までの処理手順と同様の処理手順であるので、その説明を省略する。

【００８６】ステップＳ１６０４：画像生成装置１０は、１次検証データ付き画像ファイルを検証データ変換装置２０Ａに送信する。

【００８７】ステップＳ１６０５：検証データ変換装置２０Ａは、１次検証データ付き画像ファイルを検証データ変換装置２０Ｂに送信する。

【００８８】ステップＳ１６０６：１次検証データ付き画像ファイルを受信した後、検証データ変換装置２０Ｂは、そのファイルのヘッダ部から１次検証データ及び画像生成装置１０の固有ＩＤを抽出し、そのファイルのデータ部から画像データを抽出する。また、検証データ変換装置２０Ｂは、プログラムメモリ１５２６内のテーブルＴ１を参照し、抽出された固有ＩＤに対応する共有情報Ｋｃ及び秘密情報Ｋｓを検出する。例えば、固有ＩＤが「００１」の場合、その固有ＩＤに対応する共有情報Ｋｃは「０ｘ１１１１」であり、その固有ＩＤに対応する秘密情報Ｋｓは「０ｘ２２２２」である。検証データ変換装置２０Ｂは、抽出された画像データと検出された共有情報Ｋｃとからその画像データの１次検証データを生成する。なお、検証データ変換装置２０Ｂは、画像生成装置１０と同じ生成方法に従って１次検証データを生成する。

【００８９】ステップＳ１６０７：検証データ変換装置２０Ｂは、１次検証データ付き画像ファイルから抽出された１次検証データ（即ち、画像生成装置１０の内部で生成された１次検証データ）と、ステップＳ１６０６で生成された１次検証データ（即ち、検証データ変換装置２０Ｂの内部で生成された１次検証データ）とを比較し、１次検証データ付き画像ファイル内の画像データの完全性を検証する。画像生成装置１０から検証データ変換装置２０Ｂに至るまでに改変がなかった場合、２つの１次検証データは一致し、画像データの完全性が確認される。また、同時に、検証データ変換装置２０Ｂは、この画像データが画像生成装置１０で生成された画像データであることを確実に確認することができる。この場合、検証データ変換装置２０Ｂは、改変なしと判定し、画像データの２次検証データの生成を開始する。一方、画像生成装置１０から検証データ変換装置２０Ｂに至るまでに改変があった場合、２つの１次検証データは一致せず、画像データの完全性は確認できない。この場合、検証データ変換装置２０Ｂは、改変ありと判定し、画像データが改変されていることを示すメッセージを検証データ変換装置２０Ａに送信する。なお、この場合、検証データ変換装置２０Ｂは、画像データの２次検証データの生成を禁止する。

【００９０】ステップＳ１６０８：改変なしと判定した場合、検証データ変換装置２０Ｂは、１次検証データ付き画像ファイルの画像データから２次検証データ（即ち、ディジタル署名）を生成する。なお、検証データ変換装置２０Ｂは、図８に示す生成方法に従って、画像データから２次検証データを生成する。

【００９１】ステップＳ１６０９：検証データ変換装置２０Ｂは、画像ファイルのヘッダ部にある１次検証デー

タを生成された２次検証データに置き換え、２次検証データ付き画像ファイルを生成する。生成された２次検証データ付き画像ファイルは、検証データ変換装置２０Ａに送信される。

【００９２】ステップＳ１６１０：検証データ変換装置２０Ａは、２次検証データ付き画像ファイルをインターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力する。

【００９３】ステップＳ１６１１：画像検証装置３０は、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）から２次検証データ付き画像ファイルを入力する。２次検証データ付き画像ファイルを入力した後、画像検証装置３０は、そのファイルのヘッダ部から２次検証データ及び画像生成装置１０の固有ＩＤを抽出する。また、画像検証装置３０は、プログラムメモリ３６内のテーブルＴ２を参照し、抽出された固有ＩＤに対応する公開情報Ｋｐを検出する。例えば、固有ＩＤが「００１」の場合、その固有ＩＤに対応する公開情報Ｋｐは「０ｘ１１１１」であり、その固有ＩＤに対応する秘密情報Ｋｓは「０ｘ３３３３」である。なお、公開情報Ｋｐは、所定のサーバから取得してもよい。画像検証装置３０は、抽出された２次検証データを検出された公開情報Ｋｐで復号化し、ダイジェストデータ（ハッシュ値）を復元する。なお、公開情報Ｋｐは、検証データ変換装置２０Ｂが秘密に管理している秘密情報Ｋｓに対応する情報であり、一般に公開されている情報である。

【００９４】ステップＳ１６１２：また、画像検証装置３０は、２次検証データ付き画像ファイルのデータ部から画像データを抽出する。画像検証装置３０は、抽出された画像データをハッシュ関数Ｈ２によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数Ｈ２は、検証データ変換装置２０Ｂのハッシュ関数Ｈ２と同じハッシュ関数である。

【００９５】ステップＳ１６１３：画像検証装置３０は、ステップＳ１６１１で復元されたダイジェストデータと、ステップＳ１６１２で得られたダイジェストデータとを比較し、２次検証データ付き画像ファイル内の画像データの完全性を検証する。検証データ変換装置２０Ｂから画像検証装置３０に至るまでに改変がなかった場合、２つのダイジェストデータは一致し、画像データの完全性は確認される。また、同時に、画像検証装置３０は、この画像データが画像生成装置１０で生成された画像データであることを確実に確認することができる。この場合、画像検証装置３０は、改変なしと判定し、その判定結果をユーザに通知する。一方、検証データ変換装置２０Ｂから画像検証装置３０に至るまでに改変があった場合、２つのダイジェストデータは一致せず、画像データの完全性は検証されない。この場合、画像検証装置３０は、改変ありと判定し、その判定結果をユーザに通知する。

【００９６】ステップＳ１６１４：画像検証装置３０は、２次検証データ付き画像ファイルの改変をチェックするごとに、画像ファイルのファイル名、画像ファイルの登録日時、画像ファイルの検証日時、改変の有無などの情報を保管用メモリ３５のデータベースに登録する。このような情報を保管用メモリに登録することで、検証された２次検証データ付き画像ファイルを管理する。

【００９７】以上説明したように、第２の実施の形態における画像データ検証システムによれば、第１の実施の形態と同様に、画像生成装置１０の演算リソースの性能を大幅に向上させることなく、画像生成装置１０で生成された画像データが改変されているか否かを確実に検出することができる。また、第２の実施の形態における画像データ検証システムによれば、第１の実施の形態と同様に、画像生成装置１０にかかるコストを低減することができる。

【００９８】また、第２の実施の形態における画像データ検証システムによれば、画像生成装置１０の固有ＩＤに対応する共有情報Ｋｃ、秘密情報Ｋｓ及び公開情報Ｋｐを用いて１次検証データ及び２次検証データを検証することにより、１次検証データ付き画像ファイル内の画像データまたは２次検証データ付き画像ファイル内の画像データが画像生成装置１０で生成されたものであるか否かを確実に確認することができる。

【００９９】また、第２の実施の形態における画像データ検証システムによれば、画像生成装置１０と検証データ変換装置２０Ｂとの間を１次検証データによって安全に保護することができ、検証データ変換装置２０Ｂと画像検証装置３０との間を２次検証データによって安全に保護することができるので、システム全体の安全に運用することができる。

【０１００】また、第２の実施の形態の画像データ検証システムによれば、共有情報Ｋｃ及び秘密情報Ｋｓを保持する検証データ変換装置２０Ｂをパーソナルコンピュータなどのデータ処理装置ではなく、ＩＣカード、サーバコンピュータなどの安全性の高いデータ処理装置で実現することにより、共有情報Ｋｃ及び秘密情報Ｋｓの安全性を向上させることができる。

【０１０１】次に、図１７のフローチャートを参照し、第２の実施の形態における検証データ変換装置２０Ａの処理手順について説明する。なお、図１７に示す処理手順は、プログラムメモリ１４２６のプログラムに従って実行される。また、図１７に示す処理手順は、１次検証データ付き画像ファイルを入力するごとに実行される。

【０１０２】ステップＳ１７０１：インターフェース部Ａ１４２３は、画像生成装置１０からの１次検証データ付き画像ファイルを受信する。

【０１０３】ステップＳ１７０２：インターフェース部

Ｂ１４２４は、１次検証データ付き画像ファイルを検証データ変換装置２０Ｂに送信する。

【０１０４】ステップＳ１７０３：検証データ変換装置２０Ｂが１次検証データ付き画像ファイル内の完全性を検証できなかった場合、ステップＳ１７０４に進む。一方、検証データ変換装置２０Ｂが１次検証データ付き画像ファイル内の完全性を検証できた場合、ステップＳ１７０５に進む。

【０１０５】ステップＳ１７０４：この場合、インターフェース部Ｂ１４２４は、画像データが改変されていることを示すメッセージを受信する。制御／演算部１４２１は、画像データが改変されていることを示すメッセージをユーザに通知する。

【０１０６】ステップＳ１７０５：この場合、インターフェース部Ｂ１４２４は、２次検証データ付き画像ファイルを受信する。

【０１０７】ステップＳ１７０６：インターフェース部Ｃ１４２８は、２次検証データ付き画像ファイルをインターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力する。

【０１０８】次に、図１８のフローチャートを参照し、第２の実施の形態における検証データ変換装置２０Ｂの処理手順について説明する。なお、図１８に示す処理手順は、プログラムメモリ１５２６の検証プログラムに従って実行される。また、図１８に示す処理手順は、１次検証データ付き画像ファイルを入力するごとに実行される。

【０１０９】ステップＳ１８０１：インターフェース部１５２４は、検証データ変換装置２０Ａからの１次検証データ付き画像ファイルを受信する。

【０１１０】ステップＳ１８０２：制御／演算部１５２１は、１次検証データ付き画像ファイルのヘッダ部から１次検証データを抽出する。

【０１１１】ステップＳ１８０３：また、制御／演算部１５２１は、１次検証データ付き画像ファイルのヘッダ部から画像生成装置１０の固有ＩＤを抽出し、そのファイルのデータ部から画像データを抽出する。制御／演算部１５２１は、プログラムメモリ１５２６内のテーブルＴ１を参照し、抽出された固有ＩＤに対応する共有情報Ｋｃ及び秘密情報Ｋｓを検出する。制御／演算部１５２１は、抽出された画像データと検出された共有情報Ｋｃとからその画像データの１次検証データを生成する。

【０１１２】ステップＳ１８０４：制御／演算部１５２１は、ステップＳ１８０２で抽出された１次検証データ（即ち、画像生成装置１０の内部で生成された１次検証データ）と、ステップＳ１８０３で生成された１次検証データ（即ち、検証データ変換装置２０Ｂの内部で生成された１次検証データ）とを比較し、１次検証データ付き画像ファイル内の画像データの完全性を検証する。２つの１次検証データの一致が検出された場合、ステップＳ１８０６に進む。一方、２つの１次検証データの一致が検出されなかった場合、ステップＳ１８０５に進む。

【０１１３】ステップＳ１８０５：この場合、制御／演算部１５２１は、改変ありと判定し、画像データが改変されていることを示すメッセージを検証データ変換装置２０Ａに送信する。なお、この場合、検証データ変換装置２０Ｂは、２次検証データの生成を禁止する。

【０１１４】ステップＳ１８０６：この場合、制御／演算部１５２１は、１次検証データ付き画像ファイルの画像データから２次検証データ（即ち、ディジタル署名）を生成する。

【０１１５】ステップＳ１８０７：制御／演算部１５２１は、画像ファイルのヘッダ部にある１次検証データを生成された２次検証データに置き換え、２次検証データ付き画像ファイルを生成する。生成された２次検証データ付き画像ファイルは、検証データ変換装置２０Ａに送信される。

【０１１６】以上の処理手順により、検証データ変換装置２０Ｂは、画像生成装置１０の演算リソースの性能を大幅に向上させることなく、画像生成装置１０で生成された画像データが改変されているか否かを確実に検出することができるので、画像生成装置１０にかかるコストを低減することができる。また、検証データ変換装置２０Ｂは、１次検証データ付き画像ファイルの画像データが画像生成装置１０で生成されたものであるか否かを確実に確認することができる。また、１次検証データ付き画像ファイルの完全性が確認できれば、そのファイルを２次検証データ付き画像ファイル（即ち、ディジタル署名付き画像ファイル）に変換することもできる。

【０１１７】なお、上記の各実施の形態は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０１１８】

【発明の効果】以上説明したように、本発明によれば、ディジタルカメラなどの画像生成装置にかかるコストの増大を防ぎつつ、画像生成装置で撮影された画像データが改変されているか否かを確実に検出することができる。

【図面の簡単な説明】

【図１】第１の実施の形態における画像生成装置１０の主要な構成を説明するブロック図である。

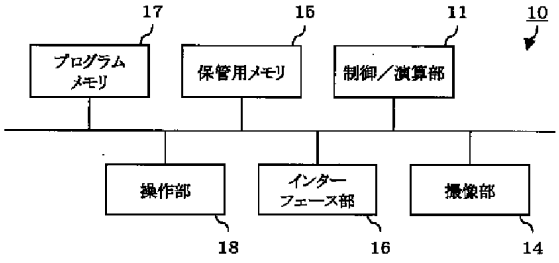
【図２】第１の実施の形態における検証データ変換装置２０の主要な構成を説明するブロック図である。

【図３】第１の実施の形態における画像検証装置３０の主要な構成を説明するブロック図である。

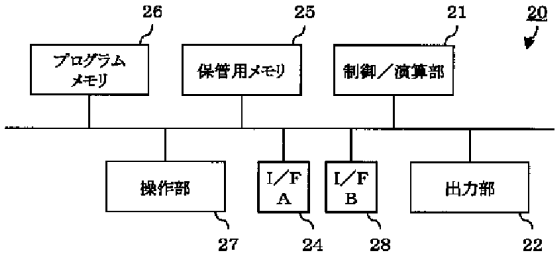
【図４】第１の実施の形態における画像データ検証シス

テムの処理手順を説明する図である。
【図５】１次検証データの生成方法の一例を説明する図である。
【図６】簡易な演算の一例を説明する図である。
【図７】テーブルＴ１及びテーブルＴ２の一例を示す図である。
【図８】２次検証データ（即ち、ディジタル署名）の生成方法を説明する図である。
【図９】第１の実施の形態における画像生成装置１０の処理手順を説明するフローチャートである。
【図１０】第１の実施の形態における検証データ変換装置２０の処理手順を説明するフローチャートである。
【図１１】第１の実施の形態における画像検証装置３０の処理手順を説明するフローチャートである。
【図１２】第１の実施の形態における画像データ検証システムの構成の一例を説明する図である。
【図１３】第２の実施の形態における画像データ検証システムの構成の一例を説明する図である。
【図１４】第２の実施の形態における検証データ変換装置２０Ａの主要な構成を説明するブロック図である。
【図１５】第２の実施の形態における検証データ変換装置２０Ｂの主要な構成を説明するブロック図である。
【図１６】第２の実施の形態における画像データ検証システムの処理手順を説明する図である。
【図１７】第２の実施の形態における検証データ変換装置２０Ａの処理手順を説明するフローチャートである。
【図１８】第２の実施の形態における検証データ変換装置２０Ｂの処理手順を説明するフローチャートである。
【符号の説明】
１０　画像生成装置
２０　検証データ変換装置
３０　画像検証装置
２０Ａ　第１の検証データ変換装置
２０Ｂ　第２の検証データ変換装置

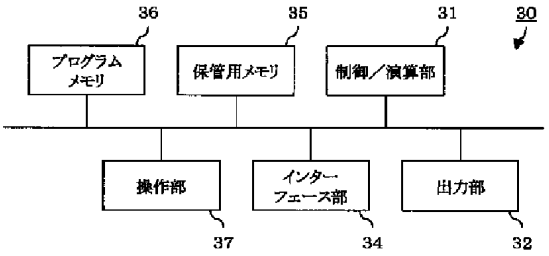
【図１】



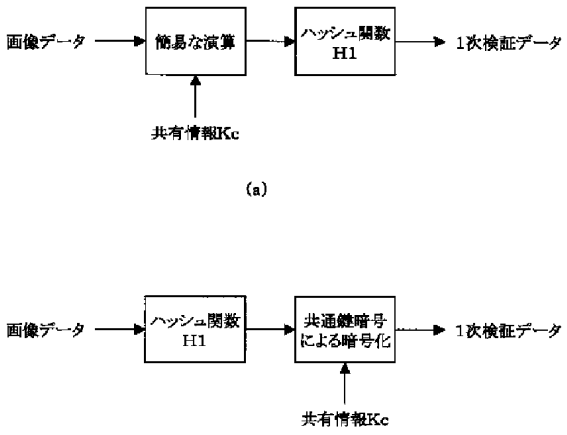
【図２】



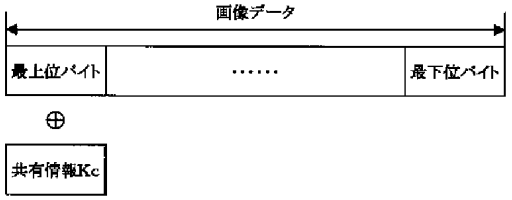
【図３】



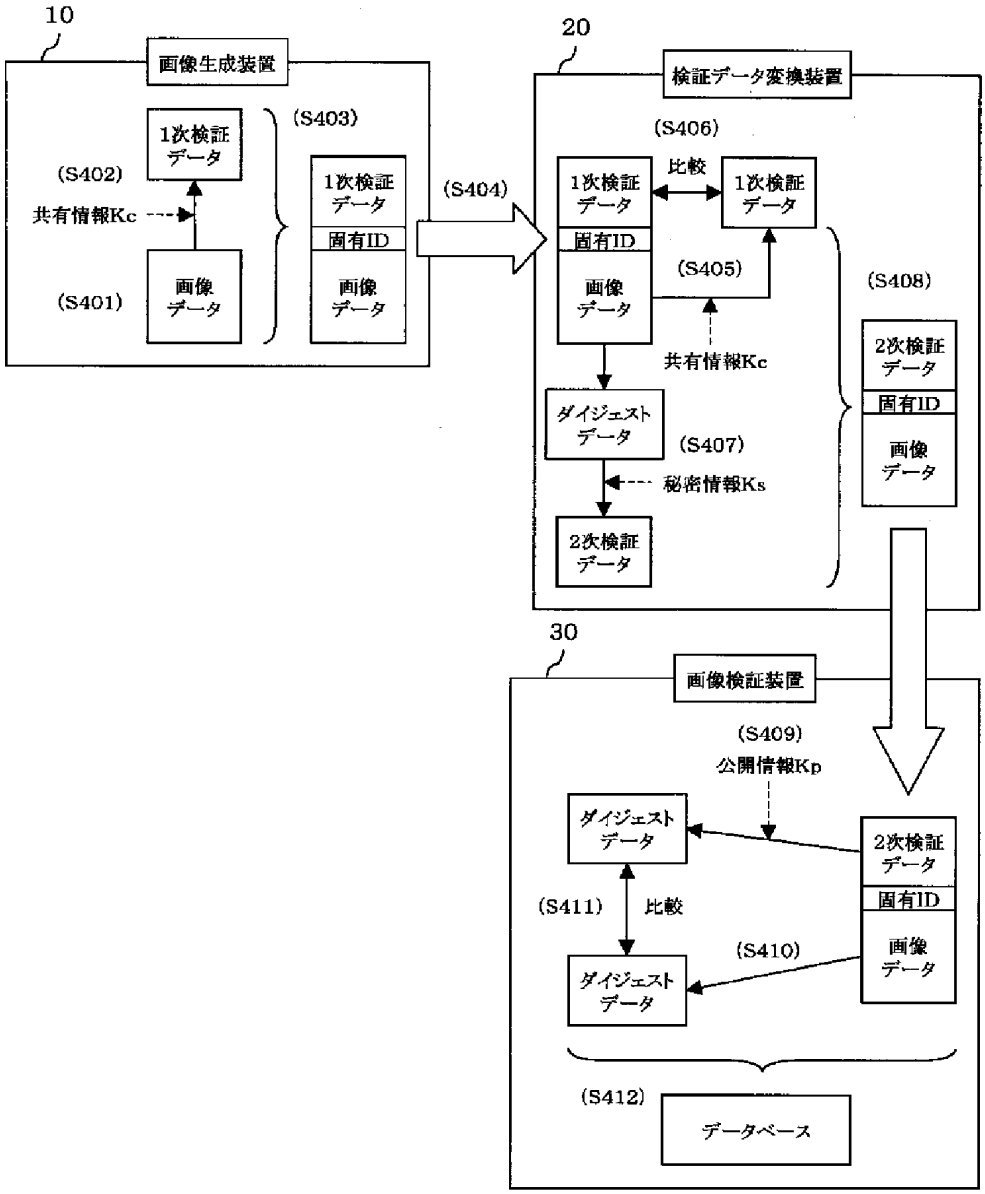
【図５】



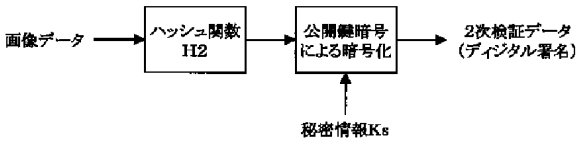
【図６】



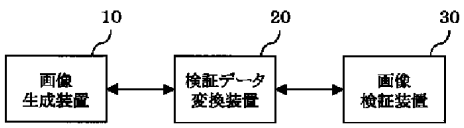
【図４】


10
画像生成装置
1次検証データ
(S403)
(S402)
共有情報Kc
(S401)
画像データ
1次検証データ
固有ID
画像データ
(S404)
20
検証データ変換装置
(S406)
1次検証データ
比較
1次検証データ
固有ID
画像データ
(S405)
共有情報Kc
(S408)
2次検証データ
固有ID
画像データ
ダイジェストデータ
(S407)
秘密情報Ks
2次検証データ
30
画像検証装置
(S409)
公開情報Kp
ダイジェストデータ
2次検証データ
固有ID
(S411)
比較
(S410)
画像データ
ダイジェストデータ
(S412)
データベース

【図８】


画像データ
ハッシュ関数
H2
公開鍵暗号
による暗号化
2次検証データ
(ディジタル署名)
秘密情報Ks

【図１２】


10
20
30
画像
生成装置
検証データ
変換装置
画像
検証装置

【図７】

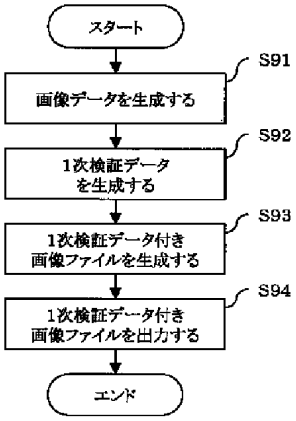
固有ID	共有情報Kc	秘密情報Ks
001	0x1111	0x2222
002	……	……
……	……	……

(a)

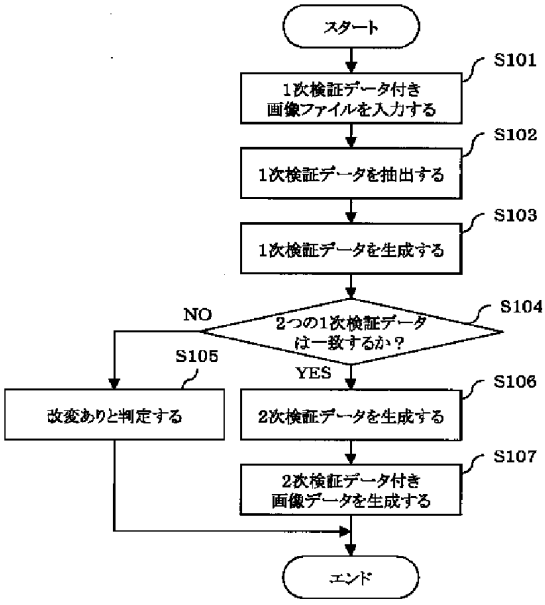
固有ID	公開情報Kp
001	0x3333
002	……
……	……

(b)

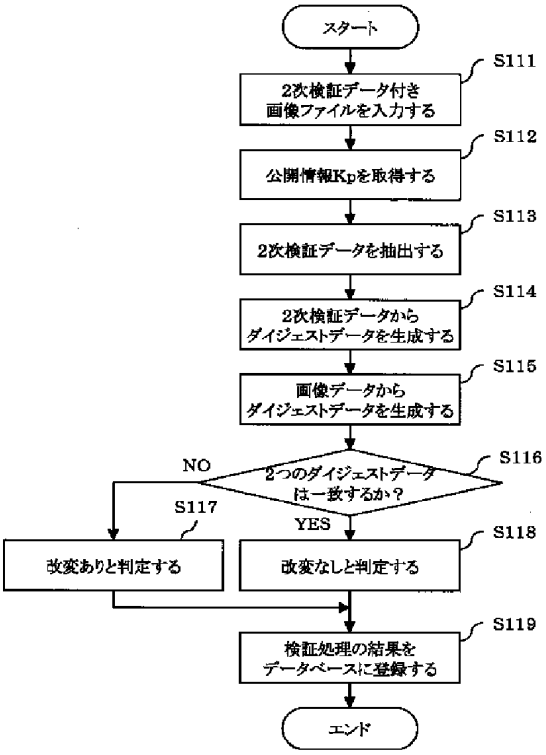
【図９】



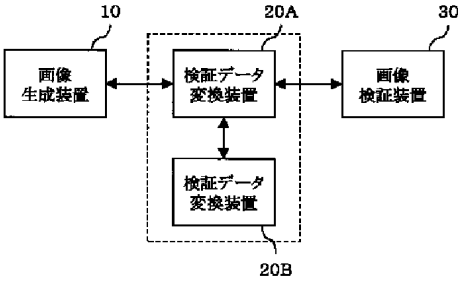
【図１０】



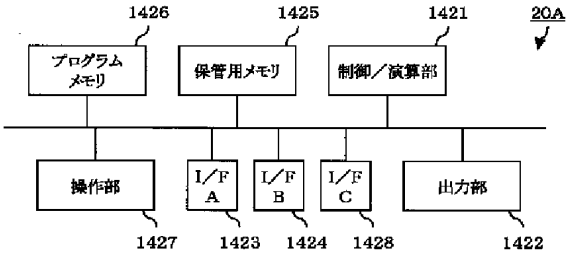
【図１１】



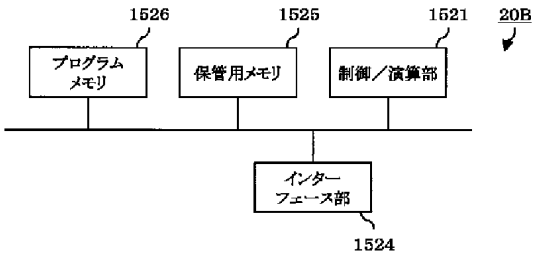
【図１３】



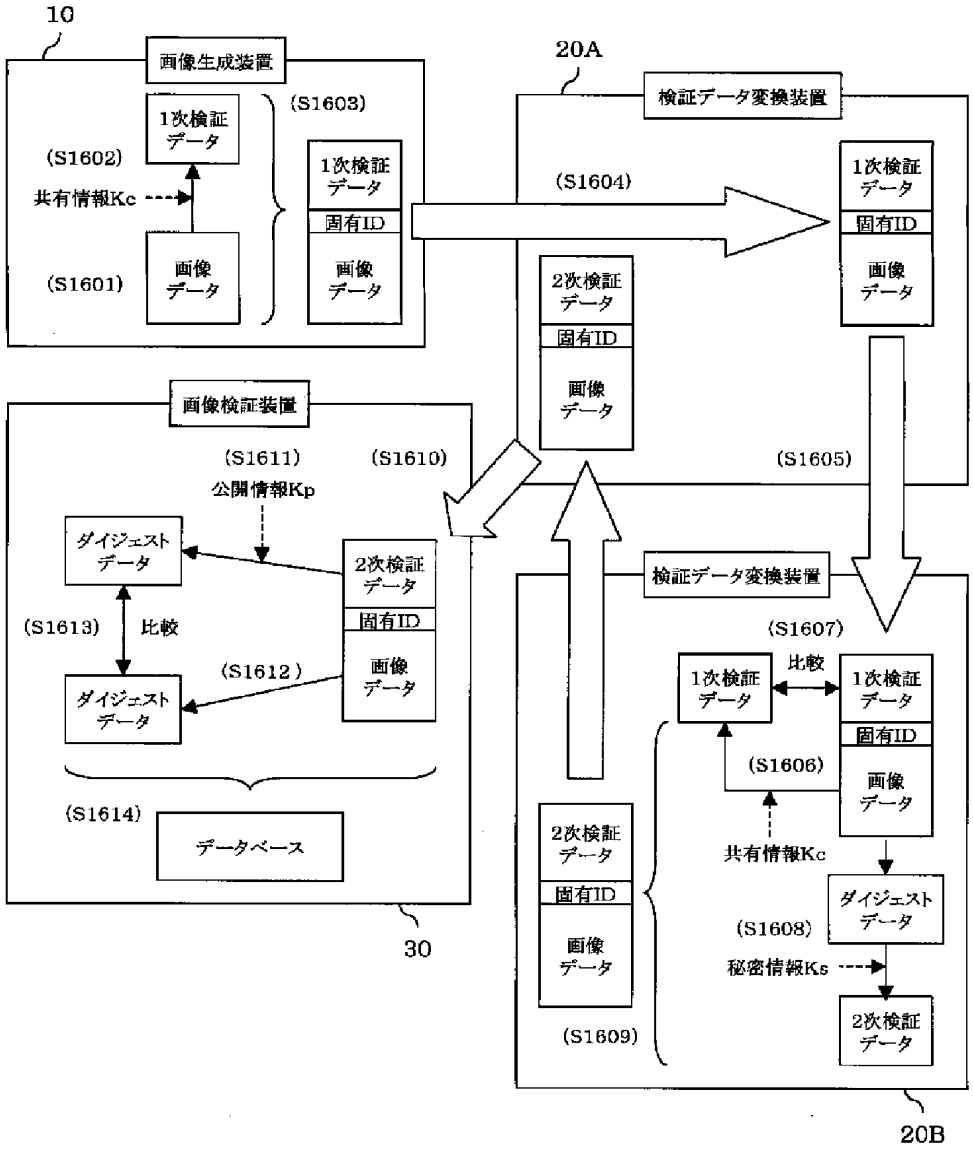
【図１４】



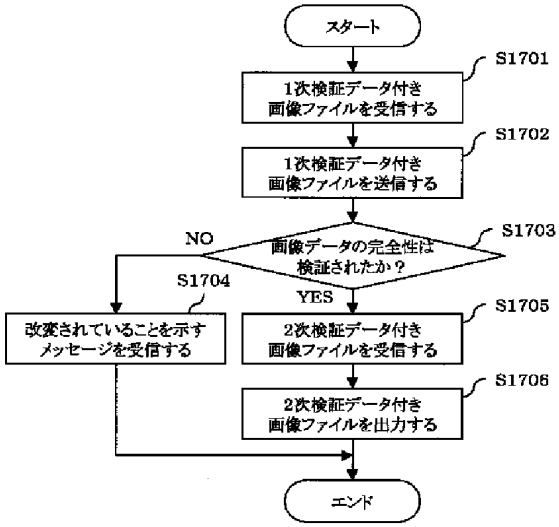
【図１５】


1526
1525
1521
20B
プログラムメモリ
保管用メモリ
制御／演算部
インターフェース部
1524

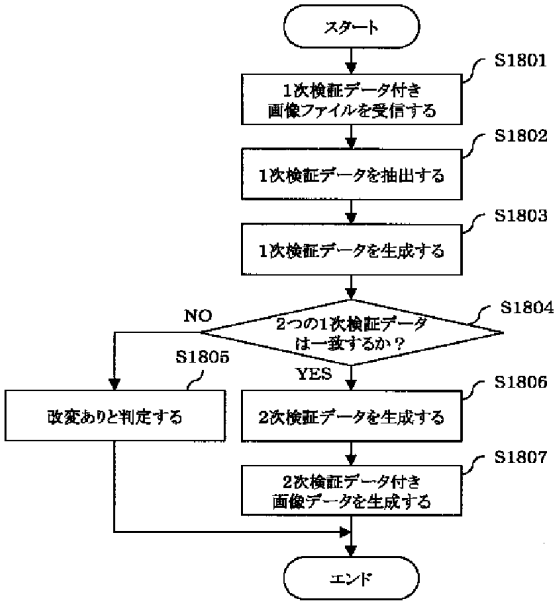
【図１６】


10
画像生成装置
(S1603)
1次検証データ
(S1602)
共有情報Kc
(S1601)
画像データ
1次検証データ
固有ID
画像データ
20A
検証データ変換装置
(S1604)
1次検証データ
固有ID
画像データ
2次検証データ
固有ID
画像データ
画像検証装置
(S1611)
(S1610)
公開情報Kp
(S1605)
ダイジェストデータ
2次検証データ
固有ID
画像データ
(S1613)
比較
(S1612)
ダイジェストデータ
(S1614)
データベース
30
検証データ変換装置
(S1607)
1次検証データ
比較
1次検証データ
固有ID
画像データ
(S1606)
共有情報Kc
2次検証データ
固有ID
画像データ
(S1608)
ダイジェストデータ
秘密情報Ks
2次検証データ
(S1609)
20B

【図１７】



【図１８】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
// Ｈ０４Ｎ 101:00		Ｈ０４Ｎ	1/40	Ｚ

Ｆターム(参考) 5B017 AA07 BA09 CA16
5C022 AA13 AC69
5C077 LL14 MP01 PP55 PQ12 PQ20
RR21 TT09
5J104 AA09 LA03 LA05 LA06 NA02